
UNITED STATES DISTRICT COURT FOR THE DISTRICT OF UTAH
CENTRAL DIVISION

EAGLE VIEW TECHNOLOGIES, INC., and
PICTOMETRY INTERNATIONAL CORP.,

Plaintiffs,

v.

NEARMAP US, INC.,

Defendant.

**DOCUMENT PRODUCTION
PROTOCOL ORDER**

Case No.: 2:21-cv-00283

District Judge Ted Stewart

Magistrate Judge Daphne A. Oberg

Before the court is the parties' Joint Motion for Entry of Document Production Protocol Order, (Doc. No. 57). The motion states the parties have agreed to the terms of this order for the collecting, searching, and producing of the parties' documents in this case, and intend for this order to supplement the District of Utah's Standard Protective Order. Based on the parties' stipulation, the court GRANTS the motion and ORDERS as follows:

1. Scope. The following protocol and definitions shall supplement the parties' responsibilities under the Federal Rules of Civil Procedure, and shall control the production of Documents, including electronically stored information ("ESI") in the matter of *Eagle View Technologies, Inc. et al. v. Nearmap US, Inc.*, pending in the District of Utah, Docket No. 2:21-cv-00283 ("Litigation"). Nothing herein shall enlarge or affect the proper scope of discovery in the Litigation, nor shall anything herein imply that any Documents or ESI produced under the terms of this protocol are properly discoverable, relevant, or admissible in this action or in any other litigation. Further, nothing in this agreement, including any provisions related to search methodology in section 16, shall excuse a party from searching for and producing Documents from locations (including both paper and electronic files) it knows or reasonably believes to have responsive information.

2. Definitions. The following terms shall be defined:

(a) “Document(s)” means all data compilations, correspondence, e-mails (hard copy or in digital form), memoranda, notes, desk calendars, diaries, statistics, letters, minutes, contracts, reports, studies, checks, invoices, statements, receipts, returns, warranties, guarantees, summaries, pamphlets, books, prospectuses, offers, notations of any sort of (i) conversations, (ii) telephone calls, or (iii) meetings or other communications, bulletins, magazines, publications, printed matter, photographs, computer printouts, worksheets and all drafts, alterations, modifications, changes and amendments of any of the foregoing, tapes, tape recordings, transcripts, graphic or aural records, and electronic, mechanical, electric, magnetic, or digital records or other tangible materials of whatever kind known to, and in the possession, custody, or control of the Producing Party.

(b) “Native File(s)” or “Native Format” means the format ESI was created or maintained by its associated software program. For example, Microsoft Excel produces its output as “.xls” or “.xlsx” files by default, which is the Native Format of Excel. Microsoft Word produces native files with a “.doc” or “.docx” extension, which is the Native Format of Word. Parties shall make a reasonable effort to collect, process and produce Native Files (if the Native Files are otherwise required to be produced) in a manner such that all files reflect accurate metadata associated with the creation and maintenance of the files and are not corrupted by the methods of the collection of the data.

(c) “Source Code” means information, document, or thing, or portion of any document or thing that includes human-readable programming language text that defines software, firmware, or electronic hardware descriptions of the Producing Party. Source Code includes text files containing Source Code, which shall hereinafter be referred to as “Source Code Files.” Source Code Files include, but are not limited to files containing Source Code written in C, C++, Java, assembler, VHDL, Verilog, SQL, and similar programming languages. Source Code Files further include “make” files, “include” files, script files, “link” files, and other human-readable text files used in the generation and/or building of software directly executed on a microcompressor, microcontroller, or digital signal processor (DSP). Source Code does not include operational versions of software, executable files, including binary executable files, and object code files, nor does it include tools such as compilers or linkers. To the extent that the parties agree that selected pages of the Source Code may be printed in hard copy, such Source Code shall be marked as “CONFIDENTIAL INFORMATION – SOURCE CODE including any information, document, or thing, or portion of any document or thing that includes Source Code.

(d) “Metadata” means broadly any data about data.

(e) “Static Image(s)” means a representation of ESI produced by converting a Native File into a standard image format capable of being viewed and printed on standard computer systems. A Tagged Image File Format (TIFF) image is an example of a Static Image.

(f) “Load/Unitization file” means an electronic file containing information identifying a set of paper-scanned images or processed ESI and indicating where individual pages or files belong together as documents, including attachments, and where each document begins

and ends. A Load/Unitization file will also contain data relevant to the individual Documents, for example, fielded data and information necessary for the loading of OCR or Extracted Text.

(g) “OCR” means the optical character recognition file which is created by software used in conjunction with a scanner that is capable of reading text-based documents and making such documents searchable using appropriate software.

(h) “Extracted Text” means the text extracted from a Native File and includes all header, footer, and document body information.

(i) “Receiving Party” shall mean the party receiving production of Documents in response to any request for production of document(s) pursuant to Fed. R. Civ. P. 34(a) or pursuant to initial production of documents identified in the party’s Rule 26(a) disclosures.

(j) “Producing Party” shall mean the party producing Documents in response to any request for production of documents pursuant to Fed. R. Civ. P. 34(a) or pursuant to initial production of documents identified in the party’s Rule 26(a) disclosures.

3. General Format of Production. Subject to the provisions of paragraph 4, Documents that are produced in these proceedings, whether or not such Documents are ESI, shall be produced in TIFF form, or native form where necessary, in the manner as described below. The parties may also produce color image Documents as Joint Photographic Experts Group (JPEG) files provided that the files comply with the specifications of this protocol applicable to TIFF files. Notwithstanding the foregoing provisions of this paragraph, the Parties reserve the right to request that an alternative format or method of production be used for certain Documents, if such Document is not susceptible to production in the format or methods of production addressed herein. In that event, the Receiving Party and the Producing Party will meet and confer to discuss alternative production requirements, concerns, formats, or methods.

4. Production Format. Documents shall be produced according to the following formats:

(a) Electronic Production of Paper Documents. Documents that are maintained in paper format shall be scanned as black and white images at 300 x 300 d.p.i., in a Group 4 compression single-page Tagged Image File Format (“TIFFs,” “.tiff format,” or “.tif format”) and reflect the full and complete information contained in the original Document. Documents shall also be produced with the associated OCR in accordance with 4(c). No Producing Party shall be required to ensure that the OCR is an exact duplicate of the contents of the TIFF image; and the Receiving Party shall accept the OCR in its “as is” condition.

(b) Electronically Stored Information. Except as provided in Paragraph 4(e) below, Document images shall be generated from electronic Documents in a Group 4 compression single-page “TIFF” image that reflects the full and complete information contained on the original document, together with a load file or functional equivalent specified in Paragraph 4(c) that contains the metadata as set forth in Paragraph 13, to the extent such metadata exists. In the event

a Document is redacted, the Producing Party shall withhold the redacted text for that Document and any metadata that is the subject of the redaction. The failure to withhold such text for a redacted document by a Producing Party shall not be deemed a waiver of the privilege associated with that Document. Extracted text will be provided for the non-redacted text.

(c) Load/Unitization File Structure. The Producing Party shall produce a unitization file (“load file”) compatible with Concordance or a comparable document management and review system, with delimited data files (commonly .DAT files), for all produced Documents in accordance with the following formatting:

Document Unitization Load File:

- Document productions should include a Concordance document load files.
- Metadata provided in a delimited file as described below under the subheading of “Metadata Load File.”

OCR and Extracted Text Files (.TXT Files):

- Single text file per document containing all the document’s pages
- Pages separated by form feed character
- Filenames should be of the form:
<Bates num>.txt, where <Bates num> is the BATES number of the first page in the document.

Image Files:

- Single page per image
- Single image per file
- TIFF is default FORMAT. In the event the Receiving Party requests specific documents in a format other than TIFF, the Receiving Party and the Producing Party will meet and confer with respect to such production as set forth in Paragraph 3.
- Filenames should be of the form: <Bates num>.<ext>
Where <Bates num> is the BATES number of the page, and <ext> is the appropriate extension for the image format (.jpg, .tif, .png, etc.)

(d) Resolution of Production Issues. Documents that cannot be read because of imaging or formatting problems shall be promptly identified by the Receiving Party. The Producing Party and the Receiving Party shall meet and confer to attempt to resolve problem(s), to the extent the problem(s) are within the Parties’ control.

(e) Native Format Documents. The Producing Party shall produce Microsoft Excel, Microsoft Access, video, and audio files in native format, unless there is an agreement to the contrary. Prior to producing any confidential information as defined in any applicable Protective Order entered herein in Native Format, the Producing Party and the Receiving Party

shall meet and confer to establish additional procedures, to the extent necessary, for the protection of the native information.

(i) Nothing in this Document Production Protocol shall eliminate or alter any Party's obligation to retain native format copies, including associated metadata, of all ESI produced in this litigation and original hard copy documents for all non-ESI produced in this litigation.

5. Production Media. A Producing Party shall produce Documents on a CD-ROM, DVD, external hard drive, or such other readily accessible computer or electronic media as the Producing Party and the Receiving Party may hereafter agree upon (the "Production Media"). Information that shall be identified on the face of the Production Media shall include: (1) the production date, and (2) the confidentiality notation required by the Protective Order entered in this case, if the media contains Confidential Information, as defined in the Protective Order. The face of the Production Media shall also contain the Bates Number range(s) of the Documents on the Production Media, and where not practicable to do so, may be provided in an accompanying letter. If the Producing Party encrypts or "locks" the production, the Producing Party shall provide under separate cover, an explanation of how to decrypt the files.

At the discretion of the Producing Party, Documents may be produced by File Transfer Protocol (FTP) or Secure File Transfer (SFT). When Documents are produced in this manner, the Producing Party may forego delivering the Documents to the Receiving Party on Production Media as described above.

6. Third-Party Software. To the extent that documents produced pursuant to this Document Production Protocol cannot be rendered or viewed without the use of proprietary or third-party software, the Parties shall meet and confer to minimize any expense or burden associated with the production of such documents in an acceptable format, including issues as may arise with respect to obtaining access to any such software and operating manuals which are the property of a third party.

7. Document Unitization. When scanning paper documents into Document Images as described in paragraph 4(a), they shall be unitized in a manner so as to maintain the document(s) and any attachments, as they existed in their original state, to the extent reasonably possible. For electronic documents, the relationship of documents in a document collection (e.g., cover letter and enclosures, e-mail and attachments, binder containing multiple documents, or other documents where a parent-child relationship exists between the documents) shall be maintained through the scanning or conversion process from native format to TIFF, provided however, that the Parties shall only be required to present one level of parent child relationship. Document Images generated from attachments to e-mails stored in Native Format shall be produced contemporaneously and sequentially immediately after the parent e-mail. All hard copy documents imaged and produced electronically shall include a unitization file ("load file") in accordance with paragraph 4(c).

8. Paper Documents Containing Fixed Notes. Paper Documents that contain fixed notes shall be scanned with the notes affixed, if it can be done so in a manner so as not to obstruct other content on the document. If the content of the Document is obscured by the affixed notes, the Document and note shall be scanned separately.

9. Duplicates. Where a Producing Party has more than one identical copy of an electronic document as determined through a verifiable MD5 Hash de-duplication process (*i.e.*, the documents are actual duplicates or duplicates determined by the e-discovery vendor software), the Producing Party need only produce a single copy of that document (as long as all family relationships are maintained). A Producing Party need not produce the same electronically stored information in more than one form.

10. Bates Numbering. Each Producing Party shall Bates number its production(s) as follows:

(a) Document Images. Each page of a produced Document shall have a legible, unique page identifier (“Bates Number”) electronically “burned” onto the image at a location that does not unreasonably obliterate, conceal, or interfere with any information from the source document. The confidentiality legend, if any, shall be “burned” onto each document’s image at a location that does not unreasonably obliterate or obscure any information from the source document. Redacted documents will be so identified by electronically “burning” the legend “Redacted” onto each document’s image at a location that does not unreasonably obliterate or obscure any information from the source document.

(b) Native Format Documents. Documents produced in Native Format will be produced with a placeholder TIFF image. Each TIFF placeholder will contain the Bates number and confidentiality designation, if any. Native format files shall be labeled with a Bates prefix, number, abbreviated designation under any applicable Protective Order, and original file extension. For example, a native format file named “123.xls” that is designated “CONFIDENTIAL - ATTORNEYS EYES ONLY” with Bates label XYZ000001 would be named “XYZ000001-CONF-AEO-123.XLS.”

11. File Naming Conventions. Each Document Image shall be named with the unique Bates Number for each page of document, as set forth in Paragraph 10 above.

12. Non-Convertible Files. Certain types of files such as system, program, video and sound files may not be amenable to conversion into anything meaningful in TIFF format. Non-convertible files will be produced in native format with a placeholder TIFF image. Some examples of file types that may not convert include file types with the following extensions: *.exp : *.exp *.ilk *.res *.trg *.tlh *.idb *.pdb *.pch *.opt *.lib *.cab *.mov *.mp3 *.swf *.psp *.chi *.chm *.com *.dll *.exe *.hlp *.ivi *.ivt *.ix *.msi *.nls *.obj *.ocx *.rmi *.sys *.tmp *.ttf *.vbx *.wav *.wpg *.iso *.pdb *.eps *.mpeg *.mpg *.ram *.rm *.psd *.ai *.aif *.bin *.hqx *.snd *.mpe *.wmv *.wma *.xfd. Other files may not be able to be converted to TIFF for reasons including, but not limited to password protection. If reasonable efforts to obtain useful TIFF images of these files

are unsuccessful, the Receiving Party and the Producing Party will meet and confer with respect to such production as set forth in Paragraph 3.

13. Metadata. The Producing Party shall produce the metadata information described below with each production and in the format described in Paragraph 4 above, to the extent such metadata already exists. Nothing in this paragraph shall be construed to obligate a party to create new metadata that is not already in existence at the time of collection of the document. For images generated from native electronic documents, a Producing Party shall produce with each production the following fields, where reasonably available.

	FIELD	DEFINITION	DOC TYPE
1	CUSTODIAN OR NON-CUSTODIAL SOURCE	Name of the person from whose files the document/data is being produced or name of data source location if not associated with single custodian	ALL
2	BEGINBATES	Beginning Bates Number (production number)	ALL
3	ENDBATES	Ending Bates Number (production number)	ALL
4	NATIVELINK	Field containing link to native file	ALL
5	TEXTPATH	File path for OCR or Extracted Text files	ALL
6	FROM	Sender	EMAIL
7	TO	Recipient	EMAIL
8	CC	Additional Recipients	EMAIL
9	BCC	Blind Additional Recipients	EMAIL
10	SUBJECT	Subject line of Email	EMAIL
11	BEGATTACH	First Bates number of a family range (i.e. Bates number of the first page of the parent email)	EMAIL/EDOCs
12	ENDATTACH	Last Bates number of a family range (i.e. Bates number of the last page of the last attachment)	EMAIL/EDOCs
13	DATESENT (mm/dd/yyyy)	Date sent	EMAIL
14	TIMESENT (hh:mm:ss TZ)	Time sent	EMAIL
15	FileExtension	Document extension (e.g. .doc, .pst, .ppt, .xls, .pdf)	EDOCs
16	AUTHOR	Creator of document	EDOCs
17	ORIGINALFILEPATH	File path location where document was originally saved	EDOCs
18	ORIGIN ALFILENAME	File name initially given when file was originally saved	EDOCs

	FIELD	DEFINITION	DOC TYPE
19	DATECREATED	Date (and time) file was created	EDOCS
20	DATELASTMODIFIED	Date (and time) file was last modified	EDOCS
21	HASH	The hash value or “de-duplication key” assigned to a document. PID’s for email families should also be preserved.	EMAIL/EDOCS
22	CONFIDENTIALITY	Confidentiality Designation	All Docs

14. Discovery and Admissibility. Nothing herein shall be construed to affect the discoverability or admissibility of any document or data. All objections to the discoverability or admissibility of any document or data are preserved and may be asserted at any time.

15. Privilege

(a) Consistent with Federal Rules of Civil Procedure, a Party withholding or redacting any responsive Document on the grounds of privilege, immunity, or any similar claim shall provide to the Receiving Party a log containing the information described in paragraph 15(b) (“Privilege Log”), except that:

(i) the Parties shall have no obligation to log information generated after the filing of the complaint; and

(ii) activities undertaken in compliance with the duty to preserve information (including, but not limited to, litigation hold letters) are protected from disclosure under Fed. R. Civ. P. 26(b)(3)(A) and (B). Notwithstanding the foregoing, if a party makes a good-faith assertion that specific documents should have been but were not preserved in the anticipation or conduct of litigation, the parties shall timely meet and confer in good faith to determine the appropriate scope, if any, of discovery regarding activities undertaken in compliance with the duty to preserve information or regarding the alleged failure to preserve such documents. In the event that the parties do not reach agreement, the party making the assertion may seek leave from the Court to request appropriate discovery. For avoidance of doubt, however, this paragraph does not constitute a waiver or other abrogation of the protections provided under Fed. R. Civ. P. 26, nor does it constitute any concession that activities undertaken in compliance with the duty to preserve information (and documents related to those activities) cannot be withheld on the basis of the attorney-client privilege, work product, or other immunity to the extent applicable.

(b) For each document withheld or redacted, the Privilege Log shall contain the following information: an entry number, a production number where an entry corresponds to redacted portions of a document, the author(s) of the document, the direct recipient(s) of the document, the copied recipient(s) of the document, the date on which the document was created or sent, a description of the document, and any privilege(s) asserted.

(c) To the extent E-mail is searched, any E-mail stream (i.e., a series of E-mails linked together by-email responses and forwarding) that is withheld or redacted on the grounds of privilege, immunity or any similar claim shall be logged by the most recent, i.e., top-most E-mail in the stream.

(d) Each member of a family (i.e., E-mail attaching memorandum) that is withheld or redacted on the grounds of privilege, immunity or any similar claim shall be logged in the same entry as the parent E-mail, provided that each such entry describes all attachments that are also withheld as privileged.

16. Search Methodology. The following governs the search methodologies for Producing Party's keyword searching to locate potentially responsive Documents contained in ESI. This Section shall supplement the parties' obligations under the Federal Rules of Civil Procedure and shall not excuse a party from those obligations, including the obligation to search for and produce documents from locations (including both paper and electronic files) it knows or reasonably believes to have responsive information.

(a) Each Party shall use its best efforts to filter out common system files using a commercially reasonable hash identification process. Hash values that may be filtered out during this process are located in the National Software Reference Library ("NSRL") NIST hash set list.

(b) With respect to the search terms, a conjunctive combination of multiple words or phrases (e.g., "computer" and "system") narrows the search and shall count as a single search term. A disjunctive combination of multiple words or phrases (e.g., "computer" or "system") broadens the search, and thus each word or phrase shall count as a separate search term unless they are contextually variants of the same word or phrase. Use of narrowing search criteria (e.g., "and," "but not," "w/x") is encouraged to limit the production.

(c) Search Methodology

(i) The Requesting Party may request the searching and production of custodial data from up to ten (10) individuals identified pursuant to Fed. R. Civ. P. 26(a)(1) or other individuals identified by the Requesting Party through any other means, including discovery, according to the methodology set forth herein. The Parties may jointly agree to modify these limits without the Court's leave. The Court will consider contested requests for additional individuals by the Requesting Party as the case develops and based upon the Requesting Party's showing of need. Regardless of the number of individuals whose custodial documents are searched, the Parties will cooperate to identify proper search terms and time frame (e.g., date ranges) on a custodian-by-custodian basis. The parties agree that the identification of documents using search terms shall be conducted by a third party electronic discovery vendor retained and directed by counsel of record.

(ii) To the extent a Producing Party elects to use search terms to locate ESI that may contain potentially responsive Documents for the individuals specifically identified by the Requesting Party under paragraph 15(d)(i), the Producing Party shall identify ten (10) search

terms to be applied to all custodial data. The Producing Party must provide any such search terms to the Requesting Party within seven (7) days of the Requesting Party's identification of a custodian for searching and production.

(iii) Within seven (7) days of identifying a custodian for searching and production, the Requesting Party may additionally propose up to five (5) search terms for the custodial data. The search terms shall be narrowly tailored to particular issues, and to the extent necessary, the Parties shall meet and confer to reach agreed-to search term lists and reasonable date restrictions. The Producing Party shall timely apply all the search terms proposed by both Parties to the custodial data, and shall timely provide the Requesting Party with resulting hit counts for each individual. The hit counts shall reflect the total number of documents that hit on each search term for each such individual, and shall separately identify the total number of responsive documents including all parents and attachments to documents that hit on each search term (i.e., families) for each such individual. If requested, the Producing Party shall also timely provide the Requesting Party hit counts that reflect the total number of unique documents that hit on each search term for each such individual (i.e., documents that contain only that term and no other search terms).

(iv) Within ten (10) days of the identification of a custodian for searching and production, or at a time mutually agreeable, the Parties shall timely meet and confer in good faith to determine whether the parties can agree on all search terms to be used for the custodial data to ensure that any requested searching and production of ESI is reasonable, narrowly tailored for specific and material issues in the case, does not impose an undue burden on the Producing Party, and is commensurate with the Producing Party's obligations under the Federal Rules. For example, and without limitation, in the event that a particular search term selected by the Requesting Party is resulting in an excessive volume of ESI where that term appears, or numerous "false positives" (i.e., non-responsive and/or immaterial documents), the Parties will meet and confer in an attempt to further narrow the search requests. Such narrowing may include further limiting date ranges or modifying the search terms.

(v) The Producing Party shall not unreasonably refuse additional requests by the Requesting Party to apply additional search terms for an individual where circumstances warrant additional searching, provided that such requests are narrowly tailored to the circumstances. Examples of such circumstances include, without limitation: (1) an individual having possession of information that the Requesting Party could not have anticipated with reasonable diligence to be in that individual's possession, or having possession of information that the Requesting Party could not have appreciated with reasonable diligence to be relevant, (2) material changes to the Producing Party's position on legal or factual issues, or (3) rulings or decisions of the Court, or changes in applicable law, that change the Requesting Party's needs for discovery or affect the scope of permissible discovery. The burden of showing that any additional searching is warranted shall be on the Requesting Party.

(vi) In the event of any requests to apply additional search terms pursuant to paragraph 16(d)(iv), the parties shall timely meet and confer as provided in paragraph

16(d)(iii) to ensure that any additional requested searching and production of ESI is reasonable, is narrowly tailored for specific and material issues in the case, does not impose an undue burden on the Producing Party, and is commensurate with the Producing Party's obligations under the Federal Rules.

17. Processing Specifications

(a) The Producing Party shall collect and process documents using methods that avoid spoliation of data. The Producing Party shall use the following specifications in this paragraph when converting ESI from its native format into TIFF image files prior to production.

(b) All tracked changes shall be maintained, to the extent reasonably feasible upon collection, so that all tracked changes to a document are evident.

(c) Author comments shall remain or be made visible, to the extent reasonably feasible upon collection.

(d) Presenter notes shall be made visible, to the extent reasonably feasible upon collection.

(e) To the extent reasonably feasible, auto-populated fields, with the exception of autopopulating "page-number" fields, shall be replaced with text indicating the field name. For example, auto-populating "date" fields shall be replaced with the text "DATE."

(f) To the extent documents in a foreign language are produced, processing of such documents shall be unicode-compliant.

(g) Notwithstanding the foregoing, a Producing Party may produce Documents that were produced in a prior litigation in the same manner as they were produced in that litigation (e.g., TIFF, native files, etc.). The Producing Party must identify any Documents as having been previously produced in another action and include the action for which they were produced. A Receiving Party may seek re-production of any such Documents in accordance with the processing specifications above, provided the Documents are available to the Producing Party and the request is made for good reason.

(h) As used herein, "to the extent reasonably feasible" does not obligate a Producing Party to obtain new or updated software if the Producing Party's current software is incapable of performing a particular processing specification listed in paragraph 17.

18. CONFIDENTIAL INFORMATION – SOURCE CODE

To the extent that any party wishes to obtain access to material designated as CONFIDENTIAL INFORMATION – SOURCE CODE, the following procedures shall apply:

(a) The Producing Party shall make all relevant and properly requested Source Code available for inspection on one stand-alone, non-networked personal computer running a reasonably current version of the Microsoft Windows operating systems (“Source Code Computer”). The Source Code Computer shall be locked down so that additional peripheral devices cannot be connected to the Source Code Computer by the Receiving Party. The Source Code Computer shall be configured to allow viewing and searching the Source Code, and may be configured by the Producing Party to run other mutually agreed upon operating systems, such as Linux, and software utilities for that purpose, provided that such utilities are reasonably necessary and non-destructive to the Source Code.

(b) The Source Code Computer shall be made available to a Receiving Party for the inspection of Source Code from 9 am to 5 pm local time, Monday through Friday (excluding holidays), and other days and/or times, upon reasonable request until the close of discovery in this action. Access after hours shall be permitted only on three (3) business days advanced written notice. A Source Code Computer will be provided in the San Francisco and New York offices of counsel for the Producing Party.

(c) The Source Code is to be treated as CONFIDENTIAL INFORMATION – SOURCE CODE, and the Receiving Party may not disclose the Source Code or the content of the Source Code to anyone who has not undertaken to abide by the Disclosure Agreement. No employee of the Receiving Party may access or obtain the Source Code.

(d) Only outside litigation counsel and/or outside experts or consultants retained by outside counsel for purposes of this action (provided they have signed a Disclosure Agreement) may have access to any portion of the Producing Party’s Source Code. For each day that counsel for the Receiving Party requests a review of the Source Code Computer, it must give at least two (2) business days (and at least 48 hours) notice to the counsel for the Producing Party that it will be sending individual(s) authorized to review the Source Code made available on the Source Code Computer.

(e) Proper identification of all authorized persons shall be provided prior to any access to the secure facility or the Source Code Computer. Proper identification is hereby defined as a photo identification card sanctioned by the government of a U.S. state, by the United States federal government, or by the nation state of the authorized person’s current citizenship. Access to the secure facility or the Source Code Computer may be denied, at the reasonable discretion of the Producing Party, to any individual who fails to provide proper identification.

(f) The Source Code Computer shall be equipped with a printer to print copies of the Source Code on bright yellow colored, pre-Bates numbered paper, with each sheet of paper bearing a header and footer reading “CONFIDENTIAL

INFORMATION – SOURCE CODE – DO NOT REPRODUCE OR DISSEMINATE,” which shall be provided by the Producing Party. Counsel for the Producing Party will keep the originals of these printed documents, and copies shall be made for counsel for the Receiving Party on such paper after being stamped with production numbers, either within 2 business days of the time they are requested (if fewer than 10 pages) or within 4 business days (if more than 10 pages). Counsel for the Receiving Party may request up to four (4) copies of any portion of printed Source Code. No more than 10% or 50 pages of the total Source Code for any software release, whichever is less, may be in printed form at any one time, and all printed Source Code shall be logged by the Receiving Party as noted below. Additionally, the Receiving Party shall not print any continuous block of Source Code that results in more than 10 printed pages. If necessary, the Receiving Party may request to print additional pages in excess of the 50 pages of total Source Code for a software release, or continuous blocks that exceed 10 pages, which request the Producing Party shall not unreasonably deny. No electronic copies of the Source Code shall be provided by the Producing Party beyond the Source Code Computer. The Producing Party shall maintain a Source Code access log identifying, for each and every time any Source Code is viewed, accessed, or analyzed: (1) the name of each person who accessed the Source Code; (2) the date and time of access; (3) the length of time of access; and (4) whether any hard copies of any portion of Source Code were printed.

(g) The Receiving Party’s outside litigation counsel of record, experts or consultants shall maintain and store any paper copies of the Source Code or any notes, analyses, or descriptions of Source Code at their offices in a manner that prevents duplication of or unauthorized access to the Source Code, including, without limitation, storing the Source Code in a locked room, cabinet, drawer or other container at all times when it is not in use.

(h) No paper copies shall be made of the printed copies of any portions of the Source Code provided by the Producing Party to the requesting party other than copies attached to sealed court filings or to be appropriately used in depositions.

(i) Except as otherwise provided within this paragraph, the Receiving Party will not create copies or duplicates or images (whether hand-copied or electronic or otherwise) of the Source Code from the paper copies for use in hard copy or on a computer (e.g., may not scan the Source Code to a .PDF or other image) or otherwise copy, save, and/or store the Source Code physically or onto any memory device or drive. The Receiving Party may only create an electronic copy or image of selected portions of the Source Code when relevant and necessary for any filing with the Court under seal, and testifying expert reports, and related drafts (hereinafter, “Selected Portions”). At least the first page of any such filing, expert report or draft containing Selected Portions shall be labeled “CONFIDENTIAL INFORMATION – SOURCE CODE” OR “HIGHLY CONFIDENTIAL

INFORMATION – SOURCE CODE – SUBJECT TO DISCOVERY CONFIDENTIALITY ORDER.” Additionally, each page containing Selected Portions shall bear a header and footer reading “HIGHLY CONFIDENTIAL INFORMATION – SOURCE CODE – DO NOT REPRODUCE OR DISSEMINATE.” The Receiving Party may not create an electronic copy or image of Selected Portions of the Source Code exceeding five (5) printed pages of code in a single document, including as an appendix to an expert report or other document. Any such electronic copy or image must be encrypted using commercially reasonable encryption software including password protection. Notwithstanding any of the foregoing, in no event shall the Receiving Party scan the paper copy of the Source Code using optical character recognition (“OCR”) technology or otherwise seek to render text-searchable any Source Code. Nor shall the Receiving Party seek to communicate electronically any copy of Source Code, except for Selected Portions, including through e-mail, FTP, or any other means of electronic communication.

(j) No outside electronic devices, including but not limited to laptops, floppy drives, USB-connectable devices, zip drives, or other hardware shall be permitted in the secure room. Nor shall any cellular telephones, Blackberries, personal digital assistants (PDAs), cameras, voice recorders, Dictaphones, telephone jacks, or other devices be permitted inside the secure room.

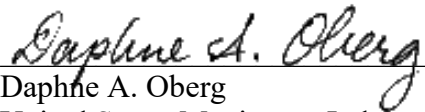
(k) The Receiving Party shall maintain a log of all copies of Source Code in its possession or in the possession of its retained experts or consultants, including the names of the recipients of any copies and the locations where the copies are stored. A copy of the log must be made available for inspection by the Producing Party at the reasonable request of the Producing Party.

(l) Within sixty (60) days after the final conclusion of this litigation, the Receiving Party must destroy all copies of the Producing Party’s Source Code. In addition, all persons to whom the copies of the Source Code were provided must certify in writing that all copies of the Source Code were destroyed or returned to the counsel who provided them the information and that they will make no use of the Source Code or of any knowledge gained from the Source Code in any future endeavor.

(m) The Receiving Party's outside litigation counsel of record, experts or consultants shall maintain and store the hard copy of selected pages of Source Code, and any notes, analyses, or descriptions of Source Code at their offices in a manner that prevents duplication of or unauthorized access to the Source Code, including, without limitation, storing the Source Code in a locked room, cabinet, drawer or other container at all times when it is not in use.

DATED this 25th day of February, 2022.

BY THE COURT:



Daphne A. Oberg
United States Magistrate Judge